CLAIM AMENDMENTS

Please amend claims 1, 7, 14, 32, 38-39, and 46-47 and cancel claims 26-31 as follows:

1. (Currently Amended) A security system reader comprising:

a transceiver that transmits a single stimulus signal to both a badge and a fingerprint keyfob and that receives a signal containing an authentication code transmitted from either the badge or the fingerprint keyfob wherein the badge and the keyfob utilize the same RF protocol; and,

a processor that is adapted to determine ~~determines~~ whether the received authentication code is from the badge or the fingerprint keyfob, and that performs an authentication of the authentication code dependent upon whether the authentication code is from the badge or from the fingerprint keyfob, wherein the authentication code from the badge is retrieved from a memory location contained within the badge and wherein the processor matches the authentication code from the badge to a list of authorized authorization codes and wherein the authentication code from the fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier, and wherein the processor is arranged to perform an authentication of the authentication code based upon both the digitized fingerprint signature and the rolling identifier in the authentication code from the fingerprint keyfob.

2. (Previously Amended) The security system reader of claim 1 wherein the processor merges the digitized fingerprint signature with the rolling identifier to form the authentication code.

3. (Previously Amended) The security system reader of claim 1 wherein the rolling identifier is provided by a rolling identifier generator.

4. (Previously Amended) The security system reader of claim 2 wherein the processor supplies the authentication code to the transceiver, which causes the authentication code to be transmitted in an RF signal.

5. (Previously Amended) The security system reader of claim 2 wherein the processor compares the digitized fingerprint signature to fingerprint signatures in a list of fingerprint signatures and also compares the rolling identifier in the authentication code from the fingerprint keyfob to an identifier maintained by the processor.

6. (Previously Amended) The security system reader of claim 5 wherein the processor compares the rolling identifier in the authentication code from the fingerprint keyfob to a rolling identifier maintained by the processor and wherein the rolling identifier is randomly or pseudorandomly generated periodically by the rolling identifier generator.

7. (Currently Amended) A method of providing access comprising:

receiving a signal containing an authentication code transmitted from either a badge or a fingerprint keyfob wherein the badge and the keyfob utilize the same RF protocol;

determining whether the authentication code is from the badge or the fingerprint keyfob <u>wherein a processer is adapted to determine if said authentication code is derived from said keyfob or said badge</u>;

determining whether the authentication code is authentic dependent upon whether the authentication code is from the badge or from the fingerprint keyfob; and,

if the authentication code is authentic, permitting access, wherein the authentication code from the fingerprint keyfob comprises a fingerprint signature and an identifier, wherein the authentication code from the badge is retrieved from a memory location contained within the badge and wherein the processor matches the authentication code from the badge to a list of authorized authorization codes and wherein the determining of whether the authentication code is authentic comprises determining whether both the fingerprint signature and the identifier in the authentication code from the fingerprint keyfob are authentic.

8. (Cancelled)

9. (Previously Amended) The method of claim 7 wherein the identifier in the authentication code from the fingerprint keyfob comprises a rolling identifier.

10. (Previously Amended) The method of claim 7 wherein the fingerprint signature comprises a digitized fingerprint signature.

11. (Previously Amended) The method of claim 7 wherein the determining of whether the authentication code is authentic comprises: comparing the fingerprint signature to fingerprint signatures in a list of fingerprint signatures; and, comparing the identifier in the authentication code from the fingerprint keyfob to a separately maintained identifier.

12. (Original) The method of claim 11 wherein the identifier in the authentication code from the fingerprint keyfob comprises a rolling identifier, and wherein the comparing of the identifier in the authentication code from the fingerprint keyfob to a separately maintained identifier comprises comparing the rolling identifier in the authentication code from the fingerprint keyfob to a separately generated rolling identifier.

13. (Original) The method of claim 7 further comprising transmitting a stimulus signal that causes at least one of the badge and the keyfob to transmit the signal containing the authentication code.

14. (Currently Amended) A method of providing access comprising:

receiving a signal containing an authentication code transmitted from either a badge or a keyfob wherein the badge and the keyfob utilize the same RF protocol;

determining whether the authentication code is from the badge or the keyfob wherein a processer is adapted to determine if said authentication code is derived from said keyfob or said badge;

determining whether the authentication code is authentic; and, if the authentication code is authentic, permitting access to a function or process; and

transmitting a stimulus signal that causes at least one of the badge and the keyfob to transmit the signal containing the authentication code, wherein the authentication code from the keyfob comprises first and second portions, wherein the first and second portions are different types of codes, and wherein the determining of whether the authentication code is authentic comprises determining whether both the first and second portions are authentic and wherein the first portion comprises a rolling identifier and wherein the authentication code form the badge comprises a single portion and the determining of whether the authentication code is authentic comprises determining whether the authentication code matches a list of authorized authorization codes.

15. (Previously Amended) The method of claim 14 further comprising providing a rolling identifier generator that generates the rolling identifier.

16. (Previously Amended) The method of claim 15 wherein the rolling identifier comprises a code that is randomly or pseudorandomly generated by the rolling identifier generator.

17. (Previously Cancelled)

18. (Previously Amended) The method of claim 14 wherein the determining of whether the authentication code is authentic further comprises:

comparing the first portion to a list; and,

comparing the second portion to a separately maintained code.

19. (Original) The method of claim 18 wherein the second portion comprises a rolling identifier, and wherein the comparing of the second portion to a separately maintained code comprises comparing the rolling identifier to a separately generated rolling identifier.

20. (Previously Amended) The method of claim 14 wherein the authentication code from the keyfob comprises a digitized fingerprint signature and an identifier, and wherein the determining of whether the authentication code is authentic comprises determining whether both the digitized fingerprint signature and the identifier are authentic.

21. (Original) The method of claim 20 wherein the identifier in the authentication code from the keyfob comprises a rolling identifier.

22. (Cancelled)

23. (Original) The method of claim 20 wherein the determining of whether the authentication code is authentic comprises:

comparing the fingerprint signature to fingerprint signatures in a list of fingerprint signatures; and,

comparing the identifier in the authentication code from the keyfob to a separately maintained identifier.

24. (Original) The method of claim 23 wherein the identifier in the authentication code from the keyfob comprises a rolling identifier, and wherein the comparing of the identifier in the authentication code from the keyfob to a separately maintained identifier comprises comparing the rolling identifier to a separately generated rolling identifier.

25. (Previously Amended) The method of claim 14 wherein the determining of whether the authentication code is from a badge or a keyfob comprises determining whether the authentication code is from a badge or a fingerprint keyfob.

26. (Cancelled)
27. (Cancelled)
28. (Cancelled)
29. (Cancelled)
30. (Cancelled)
31. (Cancelled)

32. (Currently Amended) A method for authenticating a user, comprising:

analyzing at least one RF signal containing an authentication code to determine whether the authentication code is derived from a keyfob or from a badge wherein the keyfob and the badge utilize the same RF protocol <u>wherein a processer is adapted to determine if said at least one RF signal is derived from said keyfob or said badge</u>;

processing the authentication code in a first manner if the authentication code is derived from the keyfob and constitutes a keyfob authentication code comprising a digitized fingerprint signature, in order to determine whether or not the authentication code is authentic; and

processing the authentication code in a second and different manner if the authentication code is derived from the badge wherein the authentication code from the badge is retrieved from a memory location contained within the badge and constitutes a badge authentication code, in order to determine whether or not the authentication code is authentic, and thereby grant a user access, if the authentication code is authentic.

33. (Previously Submitted) The method of claim 32 further comprising determining if the keyfob authentication code derives from the keyfob in order to process the authentication code in the first manner.

34. (Previously Submitted) The method of claim 32 further comprising determining if said badge authentication code derives from the badge in order to process the authentication code in the second and different manner.

35. (Previously Submitted) The method of claim 32 wherein processing the authentication code in a first manner if the authentication code is derived from the keyfob and constitutes a keyfob authentication code comprising a digitized fingerprint signature, in order to determine whether or not the authentication code is authentic, further comprises:

comparing the digitized fingerprint signature of the keyfob authentication code to a list of authentic digitized fingerprint signatures; and

additionally comparing a rolling identifier associated with the keyfob authentication code to a rolling identifier synchronously maintained by a processor that determines if the digitized fingerprint signature of the keyfob authentication

code matches at least one digitized fingerprint signature from among the list of authentic digitized fingerprint signatures; and

determining if the rolling identifier of the keyfob authentication code matches the rolling identifier maintained by the processor.

36. (Previously Submitted) The method of claim 32 wherein the keyfob authentication code is stored in a memory associated with the keyfob.

37. (Cancelled)

38. (Currently Amended) An access control system, comprising:

an access device; and

a plurality of authorization modules executed by a processor in association with said access device wherein said processor is adapted to determine which of said plurality of authorization modules is to be executed by said processor, wherein at least one of said plurality of authorization modules receives fingerprint data from a user in order to authorize said user to utilize said access device, wherein said fingerprint data is processed by said at least one of said plurality of authorization modules and wherein at least one other of said plurality of authorization modules receives an authorization code from a memory location.

39. (Currently Amended) The system of claim 38 ~~further comprising a processor comprising said plurality of authorization modules,~~ wherein said processor processes said fingerprint data received from said user based on an indication of whether said fingerprint data received from said user is authentic in order to permit said user to access an area or a controlled apparatus or process utilizing said access device.

40. (Previously Submitted) The system of claim 38 wherein said access device comprises a door lock.

41. (Previously Submitted) The system of claim 40 wherein said door lock comprises a stand alone push button lock that utilizes an authentication code to activate said stand alone push button lock, wherein said authentication code is changeable utilizing said processor.

42. (Previously Amended) The system of claim 38 wherein said at least one of said plurality of authorization modules comprises a keyfob reader.

43. (Previously Amended) The system of claim 42 wherein said keyfob reader comprises a fingerprint keyfob reader.

44. (Previously Submitted) The system of claim 38 wherein said at least one of said plurality of authorization modules comprises a magnetic stripe reader.

45. (Previously Submitted) The system of claim 38 wherein said data is generated by said at least one of said plurality of authorization modules based on a shared and indexed mathematical function that prevents authorizing of said data, if said data is not authorized based on a particular sequence with respect to said shared and indexed mathematical function.

46. (Currently Amended) An access control method, comprising:

providing an access device;

providing at least two types of authorization devices wherein said at least two types of authorization devices transmit data to said access device utilizing the same RF protocol;

associating a plurality of authorization modules executed by a processor with said access device wherein said processor is adapted to determine which of said plurality of authorization modules is to be executed by said processor; and

authorizing a user to utilize said access device based on said data received by said at least one of said plurality of authorization modules.

47. (Currently Amended) The method of claim 46 ~~further comprising providing a processor comprising said plurality of authorization modules,~~ wherein said processor processes said data received from said user based on an indication of whether said data received from said user is authentic in order to permit said user to access an area or a controlled apparatus or process utilizing said access device.

48. (Previously Submitted) The method of claim 46 wherein said access device comprises a door lock.

49. (Previously Submitted) The method of claim 48 wherein said door lock comprises a stand alone push button lock that utilizes an authentication code to activate said stand alone push button lock, wherein said authentication code is changeable utilizing said processor.

50. (Previously Amended) The method of claim 46 wherein said at least one of said plurality of authorization modules comprises a keyfob reader.

51. (Previously Amended) The method of claim 50 wherein said keyfob reader comprises a fingerprint keyfob reader.

52. (Previously Amended) The method of claim 46 wherein said at least one of said plurality of authorization modules comprises a magnetic stripe reader.

53. (Previously Submitted) The method of claim 46 wherein said data is generated by said at least one of said plurality of authorization modules based on a shared and indexed mathematical function that prevents authorizing of said data, if said data is not authorized based on a particular sequence with respect to said shared and indexed mathematical function.